Proposed Redacted Version of the Opposition to the Motion for Class Certification

GIBSON, DUNN & CRUTCHER LLP
LAUREN R. GOLDMAN (*pro hac vice*)
lgoldman@gibsondunn.com
DARCY C. HARRIS (*pro hac vice*)
dharris@gibsondunn.com
200 Park Avenue
New York, NY 10166-0193
Telephone: (212) 351-4000
Facsimile: (212) 351-4035

ELIZABETH K. MCCLOSKEY, SBN 268184
emccloskey@gibsondunn.com
ABIGAIL A. BARRERA, SBN 301746
abarrera@gibsondunn.com
One Embarcadero Center, Suite 2600
San Francisco, CA 94111-3715
Telephone: (415) 393-8200
Facsimile: (415) 393-8306

JONATHAN C. BOND (*pro hac vice*)
jbond@gibsondunn.com
1700 M Street, N.W.
Washington, D.C. 20036-4504
Telephone: (202) 955-8500
Facsimile: (202) 467-0539

LATHAM & WATKINS LLP
MELANIE M. BLUNSCHI, SBN 234264
melanie.blunschi@lw.com
KRISTIN I. SHEFFIELD-WHITEHEAD, SBN 304635
kristin.whitehead@lw.com
DIANNE KIM, SBN 348367
dianne.kim@lw.com
505 Montgomery Street, Suite 2000
San Francisco, CA 94111
Telephone: (415) 395-8129
Facsimile: (415) 395-8095

MARISSA ALTER-NELSON (*pro hac vice*)
marissa.alter-nelson@lw.com
1271 Avenue of the Americas
New York, NY 10020
Telephone: (212) 906-1200

JESSICA STEBBINS BINA, SBN 248485
jessica.stebbinsbina@lw.com
10250 Constellation Blvd., Suite 1100
Los Angeles, CA 90067
Telephone: (424) 653-5500
Facsimile: (424) 653-5501

Attorneys for Defendant Meta Platforms, Inc.

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE META PIXEL TAX FILING CASES

This Document Relates To:

Case No. 5:22-cv-07557-PCP, All Actions

Case No. 5:22-cv-07557-PCP (VKD)

DEFENDANT META PLATFORMS, INC.'S OPPOSITION TO PLAINTIFFS' MOTION FOR CLASS CERTIFICATION

Date: January 15, 2026
Time: 10:00 a.m.
Courtroom 8, 4th Floor

Date Action Filed: December 1, 2022
Honorable P. Casey Pitts

REDACTED VERSION OF DOCUMENT FILED UNDER SEAL

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

TABLE OF AUTHORITIES
(continued)

TABLE OF AUTHORITIES
(continued)

TABLE OF AUTHORITIES
(continued)

TABLE OF AUTHORITIES
(continued)

Page(s)

Statutes

Other Authorities

INTRODUCTION

For years, the foundational premise of this case was that Meta received "sensitive" information from TaxAct and H&R Block about the tax returns of plaintiffs and millions of other people. Based on that premise, the Court permitted the case to proceed past the pleadings stage. But discovery has revealed the premise is false. Plaintiffs have zero evidence that TaxAct or H&R Block sent *any* sensitive data about them to Meta. TaxAct sent no information about any plaintiff. And H&R Block sent only plaintiffs' browsing data—which cannot give rise to a privacy claim. *Popa v. Microsoft Corp.*, 153 F.4th 784, 791 (9th Cir. 2025).

Yet plaintiffs persist, pivoting to a new, unpled theory of the case—that Meta is liable to anyone who so much as *visited* TaxAct.com or HRBlock.com during the class period, even if they never provided (and Meta never received) any sensitive financial information. That far broader theory has no roots in the complaint or the Court's decision permitting this case to move past the pleadings. And under that new theory, plaintiffs' proposed classes contain potentially millions of uninjured people and present a host of individualized issues that could never be resolved in a class trial.

In switching to their new browsing-centric theory at class certification, plaintiffs run straight into the problems they avoided by alleging the transmission of sensitive financial information in their complaint. In particular, a claim based on the alleged sharing of browsing information does not give rise to standing, does not support a CIPA or UCL claim, and is barred by plaintiffs' consent to Meta's user agreements. Plaintiffs fall back on the alleged disclosure of their IP addresses, which they assert is "pen register" data protected under CIPA. But state legislatures cannot give litigants free passes to federal court; there can be no federal privacy suit without an actual invasion of a traditional privacy interest. *Popa*, 153 F.4th at 791–95. Internet users disclose their IP addresses to every website they visit; there is no privacy injury in the transmission of that information. Moreover, all plaintiffs and many would-be class members consented to Meta's alleged receipt of their nonsensitive data by becoming Facebook or Instagram users and agreeing to Meta's terms. For that reason, too, they cannot sue over the disclosure of data like IP addresses that is not protected private information.

The most straightforward way for the Court to approach the stark divergence between plaintiffs' sensitive-data allegations and their browsing-focused class-certification motion is to hold plaintiffs to

their complaint. Courts forbid efforts, like this one, to broaden class definitions at class certification. But it ultimately makes no difference whether the Court tackles the theory in the complaint or the one in the class-certification motion, because neither satisfies the requirements of Rule 23.

Start with typicality and adequacy. Class-action plaintiffs need to have suffered the same injury as the people they seek to represent. Plaintiffs cannot represent narrow classes of people whose financial information was sent to Meta because plaintiffs themselves did not suffer that alleged injury. And because plaintiffs are all Facebook users who agreed to Meta's policies, they would also face a consent defense that may not be available against non-users.

Nor do the proposed damages classes—either the narrower classes defined in the complaint or the broader ones defined in the motion—satisfy Rule 23's predominance requirement. Proving that any TaxAct or H&R Block website user is eligible to recover damages from Meta would require reckoning with an array of user-specific issues on an individualized basis, including:

- whether TaxAct or H&R Block sent any information about a user to Meta, let alone the sort of sensitive financial information that might give rise to Article III standing;
- whether the user implicitly consented to data sharing by learning about it and continuing to use TaxAct's or H&R Block's services, or by sharing the same information with Meta directly (such as on Facebook);
- whether the user was in California when she visited TaxAct's or H&R Block's website; and
- whether Meta received the "contents" of the user's communications.

Plaintiffs have not proposed a way to answer *any* of these questions, much less all of them, on a classwide basis. Each of these issues would require individualized analyses that would overwhelm any common questions. Courts have refused to certify classes for privacy claims based on many of these exact issues. And the only ways to get around these problems would be to deny Meta's constitutional right to litigate its defenses to individual claims, in violation of *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 366–67 (2011), or to permit TaxAct and H&R Block users to recover damages even if they are uninjured and thus lack standing, in contravention of *TransUnion LLC v. Ramirez*, 594 U.S. 413, 431 (2021). Either workaround would violate Rule 23, the Rules Enabling Act, and the Constitution.

Nor is there any basis to certify an injunctive-relief class. Plaintiffs here are focused primarily

on money; any injunction would be an afterthought. Injunctive relief would also be unnecessary: Meta has already implemented measures designed to block the receipt of potentially sensitive financial data.

Finally, a class action is not superior to individual suits. For one thing, there is no manageable way to try the sheer volume of individualized issues this case presents. For another, plaintiffs are seeking huge damages for each class member—$5,000 in statutory damages for each time a person's data was sent. That theoretical damages figure would create plenty of incentive for individual suits.

The Court should deny plaintiffs' motion for class certification.

BACKGROUND

A. Meta's Pixel helps web developers improve their websites.

Pixels are free, publicly available sets of code that website developers can customize and integrate into their websites to understand how people interact with the websites and to improve their functionality. Declaration of Tobias Wooldridge ¶ 3; Report of Dr. Georgios Zervas ¶ 15. Many tech companies, including Meta, make pixels available. Wooldridge Decl. ¶ 3; Zervas Report ¶ 13. Millions of web developers across numerous industries, including tax-filing services like TaxAct and H&R Block, use pixels. Wooldridge Decl. ¶ 3; Zervas Report ¶ 13.

Web developers choose whether to use the Meta Pixel code, where on their websites to use it, and what data to send to Meta. Wooldridge Decl. ¶¶ 3–4; Zervas Report ¶¶ 18–19. When a website visitor takes an action the developer has chosen to measure (*e.g.*, adding a product to a shopping cart), the developer sends "Event Data" about that action to Meta. Wooldridge Decl. ¶ 4; Zervas Report ¶ 18. Meta then provides analytics to the developer, helping it understand and communicate with potential customers, and the developer can choose to show ads based on the Event Data. Zervas Report ¶ 17. Developers can remove Pixel code and change what data they send at any time. *Id.* ¶ 19.

Pixel technology is widely understood. Meta's policies and many online articles describe how pixels work, and web developers (including TaxAct and H&R Block) disclose their use of pixels in their own policies. Declaration of Abbey Barrera, Exs. 1–6; Wooldridge Decl., Ex. 1. There are also many different tools and controls at users' disposal. People can prevent websites from sending data through various ad blockers, browser settings, and developer-specific controls. Zervas Report ¶¶ 83–100. And Meta provides a tool for users to see data Meta receives about them from other websites.

Barrera Decl., Exs. 7–8; Wooldridge Decl. ¶ 6. With this tool, users can also disconnect their past and/or future activity on websites from their Facebook and Instagram accounts, so that it will not be associated with them or used to show them ads. Barrera Decl., Exs. 9–10; Wooldridge Decl. ¶ 6.

B. Meta has developed tools to detect and filter out potentially sensitive financial data.

Meta does not want developers to send it any sensitive information. Barrera Decl., Ex. 11; Wooldridge Decl. ¶ 8. Meta prohibits developers from sending such information and has developed technical systems designed to prevent the receipt and use of even *potentially* sensitive data. Wooldridge Decl. ¶ 8, Ex. 1; Zervas Report ¶ 34. To use Meta's Pixel, developers must agree to terms that expressly prohibit using the Pixel code to send sensitive data, including financial data. Wooldridge Decl. ¶ 9, Ex. 1. Although the precise language has changed over time, Meta's terms also require advertisers to "warrant" that they "have all the necessary rights and permissions" for the information they share with Meta, and that they "have provided robust and sufficiently prominent notice" of their data collection that includes "how users can opt-out of the collection and use of information for ad targeting." *E.g.*, *id.*, Ex. 1 at 27–28.

Meta also devotes significant resources to developing integrity systems designed to filter out potentially sensitive terms and phrases in Event Data. Wooldridge Decl. ¶ 8; Zervas Report ¶¶ 34–35. These systems have evolved over time. Wooldridge Decl. ¶¶ 12, 16; Zervas Report ¶¶ 34–35. For example, in 2018, Meta implemented an integrity system for [redacted] Wooldridge Decl. ¶ 13; Zervas Report ¶¶ 36–38. In 2021, Meta launched a finance-specific integrity system designed to filter out other potentially sensitive financial data from [redacted] Wooldridge Decl. ¶ 14; Zervas Report ¶ 39. This system is designed to filter out potentially sensitive financial data such as [redacted]. Wooldridge Decl. ¶ 15; Zervas Report ¶ 39. And in July 2023, Meta started blocking all custom parameters and parts of URLs after the root domain from all finance-classified developers, including TaxAct and H&R Block, regardless of the data's potential sensitivity (this is referred to as "Core Setup"). Wooldridge Decl. ¶ 17; Zervas Report ¶¶ 40–43.

C. This Court denies Meta's motion to dismiss because plaintiffs allege that Meta received "sensitive financial information."

Tiffany Bryant, Katrina Calderon, Kayla Housman, Sait Kurmangaliyev, Chris Papadimitriou, and Jane Doe—Facebook users who used either or both of TaxAct's and H&R Block's tax-filing services—brought this putative class action against Meta. Dkt. 71. Plaintiffs' complaint asserted 16 claims against Meta based on tax-service providers' alleged use of the Meta Pixel to send plaintiffs' sensitive tax-filing information to Meta. *See generally id.*

Meta moved to dismiss, arguing (among other things) that Facebook users consented to Meta's receipt of their data by agreeing to Facebook's policies. *In re Meta Pixel Tax Filing Cases*, 724 F. Supp. 3d 987, 999–1000, 1003 (N.D. Cal. 2024). This Court acknowledged that "plaintiffs *could* have consented to having their data collected if they agreed to terms disclosing the practices," but held that Meta's policies do not unambiguously cover the "sensitive financial information" that plaintiffs alleged TaxAct and H&R Block shared with Meta. *Id.* at 1003–04. Specifically, the Court relied on "Meta's alleged collection of [plaintiffs'] personal financial data," including "data about income, filing status, refund amounts, and dependents' college scholarship amounts." *Id.* at 999–1000. Ultimately, the Court dismissed seven of plaintiffs' claims but permitted the other nine claims to proceed. *Id.* at 1002–26. Plaintiffs' operative complaint, which added a claim under CIPA's pen-register provision, continues to press the theory that Meta received their "sensitive financial information." Dkt. 180 ¶¶ 1, 125–35.

D. Discovery reveals the tax websites sent no sensitive financial data about any plaintiff.

Discovery did not bear out plaintiffs' allegations that the tax-filing services disclosed sensitive financial information to Meta about them; instead, it showed the opposite. [redacted] Specifically, the data matched to plaintiffs' accounts reflected that [redacted]; that [redacted] that [redacted]; and that [redacted]

[redacted]. *Id.* [redacted]. *Id.*

Discovery also revealed that, based on the sample data Meta provided, TaxAct and H&R Block rarely shared potentially sensitive financial information about *anyone*. Relying on the parameters proposed by plaintiffs' expert and taking into consideration Meta's filtering efforts, one expert determined that only [redacted] of the produced sample data sent from TaxAct to Meta via Pixel code contained even potentially sensitive financial data. Zervas Report ¶ 79. Another expert determined that, based on the sample data Meta produced, [redacted] with users active on the sites for [redacted]. Report of Dr. Steven Tadelis ¶ 28. These instances included "misclicks"—when users unintentionally click on links—and "quickbacks"—when users navigated to and then away from webpages by closing their browsers or returning to the previous page. *Id.* ¶¶ 18, 22, 26, 28. Meta's expert concluded that it was unlikely that proposed class members could have shared tax-filing information with TaxAct and H&R Block during these short website visits, and thus Meta would not have received such information in connection with those visits. *Id.* ¶ 29.

Discovery also revealed that [redacted]. *See* [redacted]; 43% of U.S. internet users regularly use ad blockers. Zervas Report ¶ 87. [redacted]. For example, [redacted]. [redacted]. And some plaintiffs testified that not all of their tax-related online activity relates to their own financial status: One plaintiff filed taxes on behalf of her mother, *id.*, Ex. 30 at 132–33, and two others [redacted], Ex. 38 at 55–56.

E. Plaintiffs move to certify classes of all visitors to TaxAct's and H&R Block's websites.

Unlike their complaint, plaintiffs' class-certification motion is not tethered to Meta's alleged receipt of "sensitive financial information." Dkt. 180 ¶ 1. Instead, plaintiffs seek to certify eight

classes of "[a]ll individuals" nationwide or in California who merely "visited the website TaxAct.com from August 25, 2015 to June 30, 2023," or "H&RBlock.com from January 15, 2019 to June 30, 2023"—regardless of whether those people provided sensitive financial information to the websites or whether the websites shared any such information with Meta. Mot. 6–7. Plaintiffs ask the Court to appoint Ms. Calderon as the sole representative for the TaxAct classes and to appoint Ms. Housman, Ms. Bryant, Ms. Calderon, and Ms. Doe as representatives for the H&R Block classes. *Id.* at i–ii.[1]

LEGAL STANDARD

A "class action is 'an exception to the usual rule that litigation is conducted by and on behalf of individual named parties only.'" *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 348 (2011). Rule 23 "imposes stringent requirements for certification that in practice exclude most claims." *Am. Express Co. v. Italian Colors Rest.*, 570 U.S. 228, 234 (2013). A plaintiff "must affirmatively demonstrate his compliance with the Rule." *Dukes*, 564 U.S. at 350. "[C]ertification is proper only if 'the trial court is satisfied, after a rigorous analysis'"—based on evidence, not pleadings or speculation—that the plaintiff has met that burden. *Id.* at 350–51. "[P]laintiffs must prove the facts necessary to carry the burden of establishing that the prerequisites of Rule 23 are satisfied." *Olean Wholesale Grocery Coop. v. Bumble Bee Foods LLC*, 31 F.4th 651, 665 (9th Cir. 2022) (en banc). And plaintiffs cannot meet that standard by proposing shortcuts: "a class cannot be certified on the premise that [the defendant] will not be entitled to litigate its statutory defenses to individual claims." *Dukes*, 564 U.S. at 367.

ARGUMENT

I. The Court should not certify classes that are broader than those defined in the complaint.

This Court should deny plaintiffs' motion because the classes they propose now are radically

[1] Plaintiffs do not advance Mr. Papadimitriou or Mr. Kurmangaliyev as class representatives. Nor do they seek certification as to any claims other than CIPA and the UCL. *See* Dkt. 180 ¶¶ 136–69, 177–97. And they do not seek certification of any claims based on TaxSlayer, another tax-service provider that the complaint alleged shared sensitive financial information with Meta. *Id.* ¶¶ 1, 4, 9, 54, 56, 60, 67, 70–73, 92, 96. Although plaintiffs' complaint alleges Meta received data unlawfully through Conversions API as well as Pixel, *id.* ¶¶ 80, 82, Conversions API is not mentioned in their class-certification motion. Plaintiffs have thus waived any arguments as to this tool. *See Zango, Inc. v. Kaspersy Lab, Inc.*, 568 F.3d 1169, 1177 n.8 (9th Cir. 2009) ("arguments not raised by a party in an opening brief are waived"). In any event, all or nearly all the same arguments presented in this brief would apply to any effort to certify a class based on data received through Conversions API.

broader than the classes they defined in their operative complaint. And their new theory of the case runs straight into the Article III standing and consent barriers they pleaded around in their complaint.

"District courts in this circuit agree that plaintiffs cannot *broaden* the class definition." *Hawkins v. Kroger Co.*, 337 F.R.D. 518, 526 (S.D. Cal. 2020). "[A] plaintiff may only seek to certify a class as defined in a complaint—courts will not certify classes different from, or broader than, a class alleged in the complaint without plaintiff moving to amend the complaint." *Richie v. Blue Shield of Cal.*, 2014 WL 6982943, at *13 (N.D. Cal. Dec. 9, 2014). Courts routinely decline to certify classes that are broader than those alleged in the plaintiffs' complaint. *E.g.*, *Turner v. Apple, Inc.*, 2025 WL 1953697, at *1–2 (N.D. Cal. July 16, 2025); *Guzman v. Polaris Indus., Inc.*, 2024 WL 5516303, at *3 (C.D. Cal. Aug. 30, 2024). That rule makes sense. The class action is just a "method[] for bringing about aggregation of claims," *Sprint Commc'ns Co. v. APCC Servs., Inc.*, 554 U.S 269, 291 (2008), and cannot expand or curtail the substantive rights of litigants, *Dukes*, 564 U.S. at 367.

Plaintiffs' motion breaks this rule by seeking certification of classes far broader than those defined in their complaint. There, plaintiffs defined the classes to include people "whose *tax filing information* was obtained by Meta from an online tax preparation provider." Dkt. 180 ¶ 92 (emphasis added). This Court permitted plaintiffs' claims to survive dismissal based on allegations that Meta received their "sensitive financial information." *Meta Tax*, 724 F. Supp. 3d at 1003–04. But now, plaintiffs seek to certify classes encompassing "[a]ll individuals" who merely "visited" TaxAct.com (between 2015 and 2023) or HRBlock.com (between 2019 and 2023)—even if they never provided any tax-filing information and even if the websites never sent such information to Meta. Mot. 6–7.

If plaintiffs presented that web-browsing-only theory in an amended complaint, they would never recover for two independent reasons. *First*, not every disclosure of web-browsing information gives rise to Article III standing. In *Popa v. Microsoft Corp.*, 153 F.4th 784 (9th Cir. 2025), the Ninth Circuit held that the plaintiff lacked standing to sue the defendant for tracking her activity on a pet-supplies website. Without allegations that "embarrassing, invasive, or otherwise private information" about the plaintiff was sent, the disclosure of this web-browsing data could not have caused any concrete injury. *Id.* at 791; *accord Daghaly v. Bloomingdales.com, LLC*, 2024 WL 5134350, at *1–2 (9th Cir. Dec. 17, 2024). Many district courts in this Circuit have similarly held that there is no legally

protected interest in web-browsing and device data.[2] Both CIPA and the UCL also require injury to bring a claim. Cal. Penal Code § 637.2(a); Cal. Bus. & Prof. Code § 17204.

Second, Meta's policies (which apply to all Facebook and Instagram users, including plaintiffs) clearly disclose, and thus establish consent for, Meta's "practices of (a) collecting its users' data from third-party sites and (b) later using the data for advertising purposes." *Smith v. Facebook, Inc.*, 745 F. App'x 8, 9 (9th Cir. 2018); *accord Meta Tax*, 724 F. Supp. 3d at 1003 ("Meta is correct that plaintiffs could have consented to having their data collected if they agreed to [Meta's Terms and Privacy Policy] disclosing the practices.") (emphasis omitted); *see also* Declaration of Michael Duffey, Exs. 1–4. This Court carved out an exception to that consent for "sensitive financial data."[3] *Meta Tax*, 724 F. Supp. 3d at 1003. But the theory behind plaintiffs' proposed classes is not tethered to sensitive financial data, and it is clear that Meta's policies establish consent for Meta to receive basic web-browsing data.

In short, plaintiffs evidently decided they could not deliver what they promised in their complaint—classes of people whose sensitive financial information was shared with Meta. But they cannot solve that problem by redefining and expanding the scope of the classes to include people who would lack Article III standing to sue and who expressly consented to the data sharing plaintiffs challenge. This Court should reject plaintiffs' eleventh-hour attempt to expand their proposed classes.[4]

---

[2] *See, e.g.*, *Khamooshi v. Politico LLC*, 2025 WL 2822879, at *2–4 (N.D. Cal. Oct. 2, 2025) (no standing to sue over collection of "browsing activity" and other device information); *Kishnani v. Royal Caribbean Cruises Ltd.*, 2025 WL 1745726, at *1, 4 (N.D. Cal. June 24, 2025) (no standing to assert CIPA pen-register claim based on collection of device, browser, and geographic information, as well as referral and URL tracking); *Carolus v. Nexstar Media Inc.*, 2025 WL 1338193, at *1 (N.D. Cal. Apr. 9, 2025) (no standing to sue over collection of "IP addresses," "the fact that a given device visited [a] website," and "the general location of that device"); *Mikulsky v. Noom, Inc.*, 682 F. Supp. 3d 855, 864–65 (S.D. Cal. 2023) (no standing unless "sensitive personal information" collected); *Lightoller v. Jetblue Airways Corp.*, 2023 WL 3963823, at *4 (S.D. Cal. June 12, 2023) (no standing where defendant recorded mouse clicks and keystrokes on its travel site).

[3] Meta respectfully disagrees and maintains that users who agreed to its terms and policies consented to even their allegedly sensitive data being sent to Meta.

[4] This Court should reject plaintiffs' overbroad class definition for another reason: it reflects claims that were never asserted in this case and would now be untimely. CIPA has a one-year statute of limitations. Cal. Civ. P. Code § 340. Plaintiffs themselves could not bring new claims years after the conduct they challenge. Nor could absent putative class members. Although tolling may permit absent class members to raise claims in an individual suit should this one falter, those absent class members could raise only the *same* claims brought here. *See Am. Pipe & Constr. Co. v. Utah*, 414 U.S. 538, 553–55 (1974) (tolling rule for class actions applies only where defendants were on notice "of the

II. The proposed class representatives are inadequate and atypical.

Whether the Court holds plaintiffs to the class definition proposed in their complaint or permits them to expand the case to all visitors to the tax-preparation sites, there is another straightforward reason to deny certification: Not a single plaintiff is a typical and adequate representative of either the alleged or the proposed classes.

1. The proposed representatives neither possess the same interest nor suffered the same injury as other class members.

For a class representative to be "typical" and "adequate," he must "possess the same interest and suffer the same injury" as the rest of the putative class. *Dukes*, 564 U.S. at 348–49 & n.5 (the requirements for typicality "tend to merge with the adequacy of representation requirement"). Here, to show that they suffered an injury, plaintiffs would need to prove (1) TaxAct or H&R Block sent information about them to Meta, and (2) that information is "sensitive" enough to be actionable. But it turns out that *not one* of the four proposed class representatives satisfies both parts of that test.

Ms. Calderon and Ms. Housman do not satisfy the first part. [redacted]. Without any data sent to Meta, a plaintiff suing over purported violations of privacy would not have a claim—and certainly could not represent a class of people whose information *was* shared. *See Griffith v. TikTok, Inc.*, 2024 WL 4308813, at *9 (C.D. Cal. Sep. 9, 2024), *appeal pending*, No. 25-553 (9th Cir.) ("because the named Plaintiffs have not produced evidence of any data collected from them, it is not even clear that they have suffered any cognizable injury, while it appears that at least some class members may have"); *Lineberry v. AddShoppers, Inc.*, 2025 WL 1533136, at *1, 6–10 (N.D. Cal. May 29, 2025) (denying class certification on typicality and adequacy grounds because of lack of data about plaintiffs). [redacted]. So she also is not an adequate or typical representative for a class of people supposedly injured by the [redacted]. *See Griffith*, 2024 WL 4308813, at *9.

substantive claims being brought against them," as well as "the number and generic identities of the potential plaintiffs who may participate in the judgment"). Plaintiffs never asserted claims premised on mere browsing of websites, and it is too late for them or anyone else to assert those claims now.

Although H&R Block did send information associated with [redacted] none of it was *sensitive*. [redacted]. Barrera Decl., Exs. 12–13; Zervas Report ¶ 80; *see supra* 5–6. [redacted].

None of the plaintiffs suffered *any* injury in fact; they certainly did not suffer the *same* injury as anyone whose sensitive financial information was actually sent. As a result, plaintiffs are not fit to represent *any* class. *See Griffith*, 2024 WL 4308813, at *8 (plaintiffs atypical because they had no "evidence[] that Defendants ever obtained any particularly sensitive information about them"); *Farley v. Lincoln Benefit Life Co.*, 150 F.4th 1197, 1203–05 (9th Cir. 2025) (plaintiff could not represent policyholders who suffered different injury); *Freeman v. Progressive Direct Ins. Co.*, 149 F.4th 461, 467 (4th Cir. 2025) (plaintiff lacked standing to sue insurer, and "without standing, [her] claim cannot be typical of the class members' claims").

2. Plaintiffs, as Facebook users, are subject to Meta's express-consent defense.

Plaintiffs who must litigate defenses not common to all members of a proposed class are neither typical nor adequate class representatives. *See, e.g.*, *DZ Reserve v. Meta Platforms, Inc.*, 96 F.4th 1223, 1238 (9th Cir. 2024); *Lineberry*, 2025 WL 1533136, at *6. Here, plaintiffs are all Facebook users and thus subject to the defense that they expressly consented to Meta's receipt of information about them. For all non-sensitive data, that defense precludes plaintiffs' claims as a matter of law. *See supra* 8–9. For sensitive data that this Court concluded might fall outside Meta's policies, *Meta Tax*, 724 F. Supp. 3d at 1003, a jury would need to decide whether those policies establish consent—in which case this defense would bar the claims of Facebook users but not non-users, *see, e.g.*, *In re Facebook Consumer Priv. Litig.*, 402 F. Supp. 3d 767, 794–95 & n.15 (N.D. Cal. 2019) (users' consent depended on "three plausible interpretations of the contract language"). Plaintiffs are thus atypical and inadequate to represent a class including non-users because "a jury could easily find against the named plaintiffs on grounds that wouldn't apply" to non-users. *Lineberry*, 2025 WL 1533136, at *1.

III. Individualized issues would predominate over common issues in any class trial.

No matter whether the Court limits plaintiffs to the sensitive-data classes they pleaded or instead examines the web-browsing classes they now seek to certify, certification is inappropriate because

there is no way to determine whether each would-be class member has a claim without litigating a long series of individualized inquiries that would make a class trial impossible. A jury would need to resolve the following questions for each putative class member: (A) whether TaxAct or H&R Block sent the user's information to Meta, whether that information was "sensitive," and what Meta did with that information; (B) whether the user consented to that data sharing; (C) whether data was transmitted within California; and (D) whether the data Meta received about that user constitutes the "contents" of a communication. Because these issues cannot be resolved in a single proceeding and plainly predominate over any common issues, Rule 23(b)(3) forbids certification of plaintiffs' damages classes.

A. There is no classwide method of proving whether TaxAct or H&R Block sent users' information or whether that information was sensitive.

Plaintiffs' proposed classes now include everyone who so much as "visited" TaxAct.com or HRBlock.com during the class periods. Mot. 6–7. That definition would sweep a huge number of uninjured people into the classes, which is alone reason to deny certification.[5] That problem would be especially acute for the "pen-register" class: No one has standing to sue over the receipt of data like IP addresses, and a class action is not a mechanism for aggregating the claims of millions of people who could never sue on their own. *See, e.g.*, *Kohen v. Pac. Inv. Mgmt. Co.*, 571 F.3d 672, 677 (7th Cir. 2009) ("a class should not be certified if . . . it contains a great many persons who have suffered no injury at the hands of the defendant"). And under any definition of the classes, it is impossible to know without extensive individualized inquiries whether TaxAct or H&R Block sent Meta *any* data about a user, much less *sensitive financial* data.[6]

---

[5] The Supreme Court has not decided "whether every class member must demonstrate standing *before* a court certifies a class." *TransUnion*, 594 U.S. at 431 n.4. Although the Ninth Circuit rejected the view that a class may not be certified if it contains more than a de minimis number of uninjured people, *Olean*, 31 F.4th at 669, it left open the possibility that a class could not be certified if a large portion of it were uninjured and it would be difficult to determine who fits in that portion. Here, the proposed classes contain a great many uninjured members, and weeding those people out would be impossible without lengthy analyses for every class member that would predominate over any common issues.

[6] Plaintiffs' bid for certification rests on Robert Zeidman's expert report, which they claim shows that certain data is transmitted "each time a person visits a website." Mot. 2–4, 7, 13–14. As explained in Meta's concurrently filed motion, Zeidman's opinions should be excluded—another basis to deny certification. Courts routinely reject certification where, as here, plaintiffs' supposed classwide proof turns on unreliable expert testimony. *See, e.g.*, *Klein v. Meta Platforms*, 766 F. Supp. 3d 956, 967 (N.D. Cal. 2025).

1. There is no classwide method to determine how users interacted with the tax-preparation services and whether those services sent any data (let alone any sensitive data) to Meta as a result.

All plaintiffs' claims require them to show that their data was shared with Meta (*see* Cal. Penal Code §§ 631, 632, 635, and 638.51; Cal. Bus. & Prof. Code § 17200) and that the data shared was sensitive (*see supra* 8–9). Plaintiffs cannot prove either of those things on a classwide basis.

Sharing. Courts deny certification where plaintiffs cannot prove that user activity on a website uniformly resulted in the collection of user data. For example, in another case against Facebook, a proposed "class consisting of all Illinois Facebook users appearing in a photograph uploaded to Facebook" was "not viable because it pose[d] insurmountable problems with . . . predominance." *In re Facebook Biometric Info. Priv. Litig.*, 326 F.R.D. 535, 542 (N.D. Cal. 2018). "[U]ploading a photo did not necessarily result in the collection of biometric data," so "a class defined by uploaded photographs [wa]s too amorphous and potentially over-inclusive to be certified." *Id.* Another court held individualized inquiries about whether a user cleared or blocked cookies in his browser defeated predominance. *In re Hulu Privacy Litig.*, 2014 WL 2758598, at *22 (N.D. Cal. June 17, 2014). And in a case against a web developer that allegedly used the Meta Pixel to send sensitive data, the court denied class certification because the plaintiff failed "to supply any indication of the percentage of users who . . . have deployed a setting or software that could" "block the Pixel." *Martinez v. D2C, LLC*, 2024 WL 4367406, at *7–8 (S.D. Fla. Oct. 1, 2024).

This case presents the same concerns. The fact that someone visited the TaxAct or H&R Block websites does not mean any data was sent to Meta, let alone data sensitive enough to be actionable. If someone used certain private browsing modes or an ad blocker, no data would have been sent to Meta. Zervas Report ¶¶ 83–87, 97–100. [redacted] And since at least January 2023, if someone with a California-based IP address visited hrblock.com, she would have seen a pop-up banner with options to accept or decline the use of "targeted advertising technologies." Barrera Decl. ¶ 42; Zervas Report ¶ 89.[7] If she opted in, data from her next visit to the website would have been sent to Meta; if she did

[7] Another version of this consent banner appeared on H&R Block's website starting in 2020, but it is unclear whether it operated in the same way. Barrera Decl. ¶ 42. Meta served a subpoena on H&R Block requesting this information, but as of this filing, H&R Block's counsel has not provided it. *Id.*

not, no data from the visit would have been sent. Zervas Report ¶ 89.

Sensitivity. Users whose information was never sent to Meta lack standing to sue over supposed privacy violations—and the same is true of those for whom only non-sensitive information was sent. An analysis of a sample of the data revealed that most visits to TaxAct's and H&R Block's websites were [redacted]; in other words, they were mostly misclicks or quickbacks, during which website visitors were unlikely to input their financial information. Tadelis Report ¶¶ 18, 22, 26, 28. Other visits, moreover, were the work of bots, and [redacted] Zervas Report ¶¶ 53–54; Barrera Decl., Ex. 39. Plaintiffs do not offer any classwide method for weeding out misclicks, quickbacks, casual browsing, or bots from the data. And even if they did propose such a method, it would not work for most of the class period because Meta does not have data for most of the class period.[8] As a result, the only way to know for sure what users did is to ask them—defeating the purpose of a class trial.

In short, there is no classwide method of determining how users interacted with the websites and what data, if any at all, was ultimately sent to Meta. That deficiency alone is reason enough to deny certification. *See, e.g.*, *Griffith*, 2024 WL 4308813, at *5–7 (denying certification in another pixel case because plaintiffs' claims turned on individualized questions about "the nature of the information collected from each class member").

2. Even if a user's "sensitive financial information" was sent to Meta, Meta may have filtered it out.

Data that is filtered out cannot be viewed or used by Meta, and users whose data was not viewed or used by Meta do not have any claim because, as explained above, they lack a privacy injury. *See supra* 8–9.[9] The evidence shows Meta filtered out potentially sensitive information that its integrity systems detected from H&R Block and TaxAct. For example, data from October 2022 shows Meta

[8] When the initial complaint was filed in December 2022, Dkt. 1, Meta's general practice was to store data received from Meta's Pixel for ads personalization purposes for up to 180 days, Wooldridge Decl. ¶ 7. Yet plaintiffs' proposed classes stretch back to 2015 (for TaxAct) and 2019 (for H&R Block).

[9] Plaintiffs do not allege Meta could be liable just for *receiving* user data that it immediately filtered out and never examined. CIPA claims also require proof of intent to receive or use the data, and if Meta immediately filtered out sensitive data, then it could not have *intended* to receive or use it. *See* Cal. Penal Code § 631(a) ("willfully"); § 632(a) ("intentionally"); § 635 ("intended").

filtered out data from TaxAct like the values TaxAct sent for [redacted] Zervas Report ¶ 79. Because Meta's integrity systems evolved over the class period and because those systems detected and filtered out specific words, numeric values, and phrases, *supra* 4, determining whether Meta filtered out sensitive financial information for a specific user would require knowing exactly what data Meta received for that user, when, and whether Meta's integrity systems filtered anything out. There is no classwide method that can accomplish this.

3. Even if a person's "sensitive financial information" was sent to Meta, Meta may not have been able to match the information to the person's account.

To have Article III and statutory standing, plaintiffs must prove Meta received sensitive information *attributable to them*. So plaintiffs need to prove Meta not only received more than anodyne information like IP addresses, *Popa*, 153 F.4th 791, but also matched that information to a particular user. *See Cahen v. Toyota Motor Corp.*, 717 F. App'x 720, 724 (9th Cir. 2017) (no injury without allegations that collected data was "sensitive or individually identifiable to particular drivers"); *Mikulsky v. Noom, Inc.*, 2024 WL 251171, at *4–6 (S.D. Cal. Jan. 22, 2024) (explaining, in CIPA case, that "[t]he disclosure of non-individually identifiable data is insufficient to give rise to an injury-in-fact to support Article III standing"); *see also Cook v. GameStop, Inc.*, 148 F.4th 153, 158–61 (3d Cir. 2025) (similar); *Dinerstein v. Google, LLC*, 73 F.4th 502, 513–14 (7th Cir. 2023) (similar).

But for two reasons, it would take individualized inquiries to figure out whether Meta matched any data it received to a specific person's account. *First*, Meta cannot match data to anyone who does not have a Meta account (*e.g.*, Facebook)—so every user would need to confirm whether she had an account when she visited TaxAct.com or HRBlock.com. Woolridge Decl. ¶ 4; *see, e.g.*, *Griffith*, 2024 WL 4308813, at *2–3 (plaintiffs failed to show that, "from the data TikTok collects, Defendants can determine the actual identity of every non-TikTok user who visits a website with the Pixel installed"). *Second*, even for those who do have a Meta account, Meta may not be able to match data it receives to that account; whether Meta can do so depends on various factors, including what data a developer sends, whether the developer is using Meta's "advanced matching" feature, whether the user is logged into a Meta account on the device being used, and a user's own browser and account settings. Woolridge Decl. ¶ 5. Plaintiffs have thus proposed no classwide method to identify all persons who

visited TaxAct.com or HRBlock.com during the class period.

4. Even if "sensitive financial information" was sent to Meta and matched to a specific account, it may not reflect that user's own information.

To prevail on their claims, plaintiffs must show for every user that the data Meta received and matched to the user's account reflects the user's *own* sensitive financial information. *See* Cal. Penal Code § 637.2(a) (conferring cause of action on "[a]ny person *who has been injured* by a violation of" the statute) (emphasis added). Courts deny class certification if individualized inquiries are necessary to determine whether the data sent to third parties reflects a user's own information. *See* Order Denying Class Certification at 15, *McDaniel v. Meta Platforms, Inc.*, Case No. 21-cv-383231 (Cal. Super. Ct. Dec. 30, 2024) (Barrera Decl., Ex. 40) (finding individual inquiries were "necessary to determine whether the data . . . reflects a particular class or subclass member's *own* video-viewing behavior rather than the video-viewing behavior of a friend or family member who had accessed that individual's HBO account"); *Byrd v. Aaron's, Inc.*, 2017 WL 4326106, at *14 (W.D. Pa. Aug. 4, 2017) (similar), *report and recommendation adopted*, 2017 WL 4269715 (Sep. 26, 2017); *Vigil v. Muir Med. Grp. IPA, Inc.*, 84 Cal. App. 5th 197, 221–23 (2022) (individualized inquiries required to determine, for each putative class member, "whether his or her information was viewed by an unauthorized party").

This case presents the same problem: Many people used someone else's device to file taxes, logged into their Facebook or Instagram accounts on a device that someone else used to file taxes (like a shared computer), or entered or searched for tax-related information on behalf of someone else, and the only way to confirm as much would be through mini-trials. For example, [redacted] Barrera Decl., [redacted]. *See* Wooldridge Decl. ¶¶ 4–6. Other plaintiffs also admitted to searching for financial or tax-related information on their own devices on behalf of others: Ms. Bryant visited H&R Block's website in 2024 to check the price of its services for her younger siblings, Barrera Decl., Ex. 38 at 55–56, and

[redacted].

People regularly prepare taxes on behalf of others, including elderly parents and children, and the IRS provides guidance on the practice. *See Publication 947 (02/2018), Practice Before the IRS and Power of Attorney*, IRS (revised Feb. 2018), https://tinyurl.com/bdea6uu5. And family members and friends must also handle the taxes of the three million people who die each year. *Deaths and Mortality*, Nat'l Ctr. for Health Stats., https://tinyurl.com/4vdjsnps. There is no classwide method of determining whether those using the tax websites supplied their own financial information or someone else's. The only way to know is to ask them—thus defeating the premise of a class trial.

5. Even if "sensitive financial information" was sent to Meta and matched to the account of someone who visited the website, that person may not treat the information as sensitive or may have already shared it with Meta.

If someone has not treated information as private or has separately shared that same information directly with Meta, she cannot sue over the disclosure of that information. Whether a plaintiff asserting privacy claims suffered an Article III "injury squarely depends on her expectations, as an invasion of privacy requires a reasonable expectation of privacy to have been violated." *Rodriguez v. Autotrader.com, Inc.*, 2025 WL 1122387, at *2–3 (C.D. Cal. Mar. 14, 2025) (CIPA claims). And "California law . . . contemplates that certain factors personal to an individual may affect whether that individual maintained a reasonable expectation of privacy." *Hart v. TWC Prod. & Tech. LLC*, 2023 WL 3568078, at *9 (N.D. Cal. Mar. 30, 2023). For example, courts have held that "tester[s] seeking to file lawsuits for invasion of [their] privacy" were *hoping* their data would be shared and "had no expectation of privacy, and thus, no injury in fact" for Article III standing. *Rodriguez*, 2025 WL 1122387, at *2–3 (no standing to assert CIPA wiretapping or pen-register claims); *accord, e.g.*, *Byars v. Sterling Jewelers, Inc.*, 2023 WL 2996686, at *3–4 & n.4 (C.D. Cal. Apr. 5, 2023). And courts have denied class certification when "[t]he reasonable expectation of privacy of class members . . . would turn on a slew of potential factors." *In re Toll Roads Litig.*, 2018 WL 4952594, at *7 (C.D. Cal. July 31, 2018); *see also, e.g.*, *Hataishi v. First Am. Home Buyers Prot. Corp.*, 223 Cal. App. 4th 1454, 1467–68 (2014) ("the determination whether an individual plaintiff had an objectively reasonable belief that his or her conversation . . . would not be recorded will require individualized proof" as to that plaintiff's specific circumstances).

Plaintiffs themselves illustrate the point. Some do not actually think the data they allege TaxAct and H&R Block sent to Meta is sensitive. Mr. Kurmangaliyev, for example, thinks only his social security number is sensitive; there is no evidence that number was ever sent to Meta, and if H&R Block had attempted to send it, it would have been filtered out. Barrera Decl., Ex. 35 at 39; *see supra* 4–6. Although some plaintiffs say they have a more expansive view of what counts as sensitive, they shared the same information they are now suing over—"income, refund amounts, filing status, the names of dependents, and scholarship information," Dkt. 180 ¶ 1—with Meta by posting it on Facebook:

- [redacted]
- [redacted]
- [redacted]

As Mr. Papadimitriou put it, "if you post it publicly," then "you give up the expectation of privacy." *Id.*, Ex. 32 at 48. Plaintiffs cannot disclose something to the world, *through Facebook or Instagram*, and then turn around and claim Meta invaded their privacy by receiving that same fact.

B. There is no classwide method to assess whether users impliedly consented to data sharing.

Consent to the challenged data sharing would doom all of plaintiffs' claims. Under California law, one "who consents to an act is not wronged by it." Cal. Civ. Code § 3515. CIPA § 631 and § 632 also specifically require proof that an unauthorized interception or eavesdropping was done "without the consent of all parties." Cal. Penal Code §§ 631(a), 632(a). "[C]ourts have consistently held that implied consent is a question of fact that requires looking at all of the circumstances surrounding the [alleged] interceptions to determine whether an individual knew that her communications were being intercepted." *In re Gmail Litig.*, 2014 WL 1102660, at *16 (N.D. Cal. Mar. 18, 2014). And courts

often deny certification of CIPA classes where individualized consent issues predominate.[10]

Here, too, individualized issues about what TaxAct and H&R Block users sent to Meta directly, and what they knew and when they knew it, would make it impossible to resolve Meta's implied-consent defense on a classwide basis. *See, e.g.*, *Gmail*, 2014 WL 1102660, at *16–18; *Brown*, 2022 WL 17961497, at *16–19. Users implicitly consented to sharing their data in two ways. *First*, anyone who posted her sensitive financial information on Facebook or Instagram consented to share that information with Meta. *See Brown*, 2022 WL 17961497, at *19. Ms. Doe, Ms. Housman, and Ms. Calderon fit that bill because they [redacted] *See supra* 17–18. Ms. Housman even admitted that her employment information, "current financial situation," and current and anticipated income bracket are not private because she posted about them publicly and that she was comfortable sharing that information with Meta. Barrera Decl., Ex. 33 at 76–79. It was not just half of the plaintiffs who shared this sort of information; many other would-be class members did, too. For example, in one public Facebook group called "Tax Refund & Stimulus Help"—which contains more than 100,000 members—potential class members posted, under their own names, about their adjusted gross income, taxable income, and tax returns. *Id.*, Ex. 14. One person posted a picture of a document stating it contained "Sensitive Taxpayer Data" and listing part of her social security number, her income, her exemptions, and more. *Id.* Plaintiffs have identified no classwide method of screening out of the class anyone who, like plaintiffs, shared directly on Meta's platforms the very things that Meta supposedly never should have learned.

Second, anyone who learned about the challenged data sharing and continued to use the tax-filing services consented to that data sharing. Some potential class members, for example, learned about it through a 2022 article published by *The Markup* and *The Verge*, which reported that "[m]ajor tax filing services . . . have been quietly transmitting sensitive financial information to Facebook when Americans file their taxes online," including "data on users' income, filing status, refund amounts, and dependents' college scholarship amounts." Barrera Decl., Exs. 15–16. Other major news outlets,

[10] *E.g.*, *Brown v. Google, LLC*, 2022 WL 17961497, at *18–19 (N.D. Cal. Dec. 12, 2022); *In re Google RTB Consumer Priv. Litig.*, 2024 WL 2242690, at *11–14 (N.D. Cal. Apr. 4, 2024); *Gmail*, 2014 WL 1102660, at *16–19.

including CNBC, soon published their own articles, and those publications collectively reached tens of millions of readers, including [redacted]. *Id.*, Exs. 17–18, [redacted]; Declaration of Christopher Weil ¶¶ 7–8, 12–13, 17–18. For example, 7.9 million users' social-media feeds displayed the link to *The Markup* article, and CNN, with almost 200 million monthly visitors to its page, shared the article. Weil Decl. ¶¶ 7–8. Similarly, 6.5 million users' social-media feeds displayed the link to the CNBC article. *Id.* ¶ 12. Others learned about the data sharing through ads recruiting plaintiffs for this very case. Ms. Bryant and Mr. Kurmangaliyev first learned about the claims in this case after seeing such ads between 2019 and 2022. Barrera Decl., Exs. 28–29, Ex. 35 at 173–74, 254, Ex. 38 at 74–75. Despite being on notice of the alleged misconduct, both continued to use H&R Block. *Id.*, Ex. 35 at 128–29, Ex. 38 at 118. Others who similarly read an article or saw an ad and kept using TaxAct's or H&R Block's services impliedly consented to the data sharing. *See Brown*, 2022 WL 17961497, at *19. But there is no classwide method to figure out who those people are; Meta knows what plaintiffs read only because it had an opportunity to take discovery from them.

C. There is no classwide method of determining whether data was sent to or from California.

Plaintiffs' claims are all limited to activity within California, and plaintiffs have identified no method of determining in one stroke the place where all would-be class members accessed the TaxAct and H&R Block websites. CIPA § 631 is expressly limited to in-state conduct, as it forbids "read[ing], or attempt[ing] to read," a message while it is "in transit or passing over any wire, line or cable, or is being sent from, or received at any place within this state." Cal. Penal Code § 631(a). As for CIPA's other provisions, "[u]nder California law, a presumption exists against the extraterritorial application [of] state law." *O'Connor v. Uber Techs., Inc.*, 58 F. Supp. 3d 989, 1004–07 (N.D. Cal. 2014). Courts "presume the Legislature did not intend a statute to be 'operative, with respect to occurrences outside the state, . . . unless such intention is clearly expressed or reasonably to be inferred from the language of the act or from its purpose, subject matter or history.'" *Sullivan v. Oracle Corp.*, 51 Cal. 4th 1191, 1207 (2011). The Legislature has not clearly expressed any intent for CIPA to apply outside of California. And the California Supreme Court has clarified that the "principal purpose" of CIPA § 632 "is to protect the privacy of confidential communications of California residents *while they are in California*." *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95, 119–20 (2006).

Courts therefore dismiss California privacy claims where plaintiffs have not alleged they were in California when accessing a website. *See, e.g.*, *Doe v. Call-On Doc, Inc.*, 2025 WL 1677632, at *6, 11 (S.D. Cal. June 13, 2025) (dismissing CIPA claims where plaintiff was a California resident but did not allege she "was in California when she accessed Defendant's website"). And where, as here, class members' locations are essential to establishing a claim or defense, courts hold certification is inappropriate. *E.g.*, *Hale v. Emerson Elec. Co.*, 942 F.3d 401, 403–04 (8th Cir. 2019) (per curiam); *Spence v. Glock, GmbH*, 227 F.3d 308, 314–16 (5th Cir. 2000). In a recent case against Meta involving a similar tool for apps, for example, the court denied certification of a CIPA § 631 class because there was "no classwide method of determining whether California resident users" interacted with an app "while they were in California." *Frasco v. Flo Health, Inc.*, 349 F.R.D. 557, 586–87 (N.D. Cal. 2025).

Here, too, whether a user was in California when accessing tax-preparation websites and whether that user's information was received in California are highly individualized issues. Plaintiffs broadly defined the classes to include anyone who accessed the websites from anywhere in the country. So the classes will include many people who were outside of California—and therefore ineligible to recover. In fact, plaintiffs themselves accessed TaxAct's and H&R Block's websites from other states: [redacted]. Barrera Decl., Exs. 20–22, 25. Although plaintiffs initially brought wiretapping claims under their home-state statutes, they do not seek certification as to those claims. Dkt. 71 ¶¶ 113–131, 167–202. The only way to determine where other users were when they accessed the tax websites would be through user-specific discovery and cross-examination.

Plaintiffs may try to get around this individualized-location question in four ways, but none of them would be persuasive. *First*, plaintiffs might argue the California choice-of-law provision in Meta's terms "makes nationwide classes permissible here." Mot. 11. But that clause means only that California law applies, not that plaintiffs should *win* under California law, and the presumptive bar against the extraterritorial application of California law is one reason they may lose.[11] The proposed classes, moreover, include non-Facebook and non-Instagram users, who would not have any choice-

[11] *See O'Connor*, 58 F. Supp. 3d at 1005 ("[A] contractual choice of law provision that incorporates California law presumably incorporates *all* of California law—including California's presumption against extraterritorial application of its law."); *Cotter v. Lyft, Inc.*, 60 F. Supp. 3d 1059, 1065 (N.D. Cal. 2014) (choice-of-law clause "could not" confer California claim upon "out-of-state" plaintiffs).

of-law clause to invoke. If someone lacked sufficient ties to California, another state's laws may apply—which explains why plaintiffs initially brought claims under the laws of the states where they live. This choice-of-law problem defeats predominance. *See Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 589–94 (9th Cir. 2012) (vacating certification where district court "erroneously concluded that California law could be applied to the entire nationwide class"), *overruled on other grounds by Olean*, 31 F.4th at 682 n.32.

Second, plaintiffs might contend users' location is irrelevant because Meta is a California company that must have received all data in California. *See* Mot. 11. But that is not how the company operates. Meta receives data at "Points of Presence," which act like cell towers and are located around the country. Declaration of Daniel Rampton ¶¶ 5–7, 9. California is thus not where "the conduct that 'creates liability'" occurred. *Oman v. Delta Air Lines, Inc.*, 889 F.3d 1075, 1079 (9th Cir. 2018).

Third, plaintiffs say the data Meta produced includes fields that [redacted] Mot. 13–14. But those fields [redacted] Zervas Report ¶¶ 58–59; *see also Frasco*, 349 F.R.D. at 587 (plaintiffs' evidence, including code containing location names, was insufficient to show where class members were located). And VPNs, which some plaintiffs admitted using, Barrera Decl., Ex. 32 at 46, Ex. 36 at 43, can mask IP addresses and allow people to access websites with a network location other than their current location, Zervas Report ¶¶ 59–60. Like Ms. Doe and Mr. Papadimitriou, many others no doubt used VPNs that would have masked their location when accessing the websites. In 2019, at least a quarter of Americans used a VPN to access the internet; by 2023, a third of Americans always used VPNs. *Id.* ¶ 59. Individualized inquiries would thus be required to learn users' *actual* locations when they visited the TaxAct and H&R Block websites and prompted data transmissions to Meta.

Fourth, plaintiffs might fall back on the two classes that are limited to "individuals in California," but that is no answer, either. By "individuals in California," plaintiffs presumably mean California *residents*. But residents have no CIPA claim if their supposed injury happened outside of the state. *See supra* 20–21; *Call-On Doc*, 2025 WL 1677632, at *6.

D. There is no classwide method to determine whether Meta received the "contents" of particular class members' communications with TaxAct and H&R Block.

To prove their CIPA § 631 claim under either of their proposed class definitions, plaintiffs must show that Meta received the "contents" of their communications. Cal. Penal Code § 631(a). The Ninth Circuit has explained that "the term 'contents' refers to the intended message conveyed by the communication and does not include record information regarding the characteristics of the message that is generated in the course of the communication." *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). URLs reflecting the mere fact of a website visit, "as opposed to information [plaintiffs] might have entered while using the website," do not constitute "contents." *Daghaly*, 2024 WL 5134350, at *1; *see also Zynga*, 750 F.3d at 1108–09. And "keystrokes, mouse clicks, pages viewed, . . . the date and time of the visit, the duration of the visit, Plaintiff's IP address, her location at the time of the visit, her browser type, and the operating system on her device" do not qualify as "contents" either. *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082–83 (C.D. Cal. 2021); *see also Mikulsky v. Bloomingdale's LLC*, 713 F. Supp. 3d 833, 845 (S.D. Cal. 2024). And although some information (like IP addresses) can *never* qualify as contents, other information can sometimes be contents and sometimes mere metadata—and figuring out which it is requires a context-specific analysis. "[T]he line between contents and metadata is not abstract but contextual with respect to each communication." *In re Google Inc. Cookie Placement Consumer Priv.*, 806 F.3d 125, 137 (3d Cir. 2015). For example, a name would be the contents of a response to the question, "What is your name?," but would *not* be contents if it appeared in the "from" line of an email.

Here, individualized inquiries are necessary to understand the context in which anyone's data was sent to Meta—and thus whether the "contents" of their communications were transmitted. The court in *Griffith* held as much when it denied certification of a class of non-TikTok users whose information was collected by TikTok when they visited thousands of websites that used TikTok's pixel. 2024 WL 4308813, at *1. The court held individualized issues predominated because "whether a class member has had the contents of his or her communications collected" under CIPA "depends on the nature of the information collected," which varied among class members. *Id.* at *6–9. The same is true here. Plaintiffs' class definitions sweep in everyone who visited TaxAct's or H&R Block's

homepage, not just users who filed tax returns. The produced data sample revealed that most visits to the tax websites made by would-be class members were brief, with users active for [redacted] Tadelis Report ¶ 28; *see supra* 6, 14. Whether the data Meta received about class members (if any) constitutes the "contents" of a communication will depend on the type of data at issue and the context in which it was sent. *See Griffith*, 2024 WL 4308813, at *6–9. And there is no classwide method to determine the types of data and the various contexts in which that data was sent to Meta.

IV. This Court should not certify an injunctive-relief class.

Plaintiffs also ask to certify a Rule 23(b)(2) class under the UCL, Mot. 16–18, but this case is a poor fit for that relief for three reasons. The first is that, as this Court has explained, an injunctive-relief class is inappropriate where (as here) plaintiffs primarily seek money. *Rabin v. Google LLC*, 787 F. Supp. 3d 934, 954 (N.D. Cal. 2025); *see also Zinser v. Accufix Rsch. Inst., Inc.*, 253 F.3d 1180, 1195 (9th Cir. 2001) ("Rule 23(b)(2) certification is inappropriate where the primary relief sought is monetary."). Plaintiffs "acknowledge" this Court's decision denying certification in *Rabin* and "ask the Court to reconsider the issue." Mot. 16 n.2. But they have not given a compelling reason to reach a different result here, where there can be little doubt that plaintiffs are focused on money (despite having no economic or other injury). Of the eight classes plaintiffs seek to certify, *six* of them are damages classes under CIPA, seeking statutory damages of $5,000 per violation under CIPA § 637.2. And one plaintiff testified that [redacted] "Plaintiffs' request for monetary damages is not merely incidental to the request for injunctive relief." *Broadbent v. Internet Direct Response*, 2011 WL 13217499, at *4 (C.D. Cal. Feb. 2, 2011).

The second reason is that, as explained above, plaintiffs flunk the typicality and adequacy requirements that apply equally to damages and injunctive-relief classes. *See supra* 10–11; *Black Lives Matter L.A. v. City of Los Angeles*, 113 F.4th 1249, 1265 (9th Cir. 2024).

The third reason is that injunctive relief is unnecessary. At least according to the complaint, this case is about transmitting "sensitive" data from the tax websites to Meta, and there is no reason to think any such data will be sent. Meta has implemented mitigations—including Core Setup—aimed at preventing its receipt of potentially sensitive financial data, *see supra* 4, and plaintiffs' decision to end the class period in July 2023, after Meta implemented Core Setup, reflects their acknowledgment that

Core Setup addressed the issues described in their complaint. And although the tax websites may still use Pixel code to send non-sensitive information—such as whether someone has visited each website—the TaxAct and H&R Block privacy policies clearly disclose that data sharing. *See, e.g.*, Barrera Decl., Ex. 5(a) at 2–3, Ex. 5(m) at 3–5, Ex. 6(a) at 2, Ex. 6(r) at 6–9. So do Meta's policies. *See, e.g.*, Wooldridge Decl., Exs. 1–2. Those disclosures foreclose any privacy claim. *See, e.g.*, *Hammerling v. Google, LLC*, 2024 WL 937247, at *2 (9th Cir. Mar. 5, 2024) (affirming dismissal of privacy claims because defendant "disclosed the challenged data collection efforts in the Policy"). Where, as in this case, plaintiffs' requested injunctive relief is not necessary, it "cannot serve as a predicate for Rule 23(b)(2) certification." *Thorn v. Jefferson-Pilot Life Ins. Co.*, 445 F.3d 311, 331 (4th Cir. 2006); *accord, e.g.*, *Smith v. City of Oakland*, 2008 WL 2439691, at *1 (N.D. Cal. June 6, 2008).

V. A class action is not "superior" to individual suits.

Plaintiffs have not met their burden to show that "a class action is superior to individual actions in fairly and efficiently adjudicating this case," *Colman v. Theranos, Inc.*, 325 F.R.D. 629, 640 (N.D. Cal. 2018), for two reasons. *First*, plaintiffs offer no manageable way to try the pervasive individualized issues and defenses in this case. *See supra* 11–24. Litigating these issues will require evidence and jury verdicts unique to each class member. *See Lara v. First Nat'l Ins. Co. of Am.*, 25 F.4th 1134, 1140 (9th Cir. 2022) (no superiority where class action "would involve adjudicating issues specific to each class member's claim, and that would be unmanageable"). *Second*, there is "sufficient monetary incentive [for class members] to pursue their own claims." *Nguyen v. BDO Seidman, LLP*, 2009 WL 7742532, at *8 (C.D. Cal. July 6, 2009). CIPA authorizes high statutory damages—$5,000 per violation. Cal. Penal Code § 637.2(a)(1). And plaintiffs seek to multiply that figure by the number of each user's "visits to H&R Block's and TaxAct's websites." Mot. 15. Plaintiffs thus could be seeking tens or even hundreds of thousands of dollars for the average user. That amount is large enough to spur users to pursue individual cases against Meta, in which issues unique to them can be litigated. *See Nguyen*, 2009 WL 7742532, at *8 (denying certification because would-be class members were "well-paid employees . . . seeking years worth of overtime back-pay, penalties, and attorney fees").

CONCLUSION

The Court should deny plaintiffs' motion for class certification.

DATED: October 27, 2025

GIBSON, DUNN & CRUTCHER LLP

By: */s/ Lauren R. Goldman*
Lauren R. Goldman